CLAIMS

We claim:

1. A computer implemented method comprising:

determining a set of endpoints for a generic routing encapsulation (GRE) tunnel;

determining a key, the key corresponding to a virtual private network (VPN);

dynamically establishing the GRE tunnel with the set of endpoints and the key; and

processing a set of GRE traffic for the VPN.

2. The computer implemented method of claim 1 wherein the set of points comprise a first value indicating a first virtual router, the first virtual router corresponding to the VPN, a second value indicating a second virtual router, a third value indicating a third virtual router, the second and third virtual routers corresponding to a backbone, and a fourth value indicating a fourth virtual router, the fourth virtual router corresponding to the VPN.

3. The computer implemented method of claim 1 wherein dynamically establishing the GRE tunnel comprises:

establishing a first subset of the set of endpoints for entering and exiting the VPN; and

establishing an initiation point and a termination point for the GRE tunnel with a second subset of the set of endpoints.

4. A computer implemented method comprising:

determining a first set of endpoints for a generic routing encapsulation (GRE) tunnel;

determining a key, the key corresponding to a virtual private network (VPN);

using the key and the set of endpoints to determine a second set of endpoints for the VPN;

establishing the GRE tunnel with the set of attributes; and

processing a set of traffic for the VPN.

5. The computer implemented method of claim 4 wherein the first set of endpoints comprise a first value indicating a first virtual router, the first virtual router being an initiation point of the GRE tunnel, and a second value indicating a second virtual router, the second virtual router being a termination point for the GRE tunnel.

6. The computer implemented method of claim 4 wherein the second set of endpoints comprise a first value indicating a first virtual router corresponding to the VPN, and a second value indicating a second virtual router, the second virtual router corresponding to the VPN.

7. The computer implemented method of claim 4 wherein the second set of endpoints and the set of attributes are each indexed by the key and the first set of endpoints.

8. A system comprising:

a first network element to determine a key and a first set of endpoints for a generic routing encapsulation (GRE) tunnel, the key corresponding to a virtual private network (VPN), to determine a second set of endpoints for the GRE VPN, to configure an initiation point of the GRE tunnel, to transmit a packet having the first set of end points and the key; and

a second network element coupled with the first network element, the second network element to receive the packet, to determine the second set of endpoints for the GRE VPN, and to establish the GRE tunnel.

9. The system of claim 8 further comprising a third network element, the third network element coupled with the first and the second network element, the third network element to receive a set of data from the first network element and forward the set of data to the second network element, the set of data being for the VPN.

10. The system of claim 8 wherein the second set of endpoints are indexed by the first set of endpoints and the key.

11. The system of claim 8 wherein to configure the initiation point comprises to configure one of the second set of endpoints to one of the first set of endpoints.

12. An apparatus comprising:

a control engine to retrieve a first set of endpoints corresponding to a generic routing encapsulation (GRE) tunnel, to retrieve a second set of endpoints corresponding to the first set of endpoints and a key, the key corresponding to a virtual private network (VPN); and

a forwarding engine coupled with the control engine, the forwarding engine to establish an initiation point of the GRE tunnel and to transmit a set of traffic over the GRE VPN.

13. The apparatus of claim 11 wherein the forwarding engine to host a first and second virtual router, the first virtual router corresponding to one of the first set of endpoints and the second virtual router corresponding to one of the second set of endpoints.

14. The apparatus of claim 11 wherein the second set of endpoints are indexed by the key and the first set of endpoints.

15. An apparatus comprising:

an input/output module to receive a set of data, the set of data indicating a key and a first of set of endpoints of a generic routing encapsulation GRE tunnel, the key corresponding to a virtual private network (VPN); and

a control engine coupled with the input/output module, the control engine to determine a second set of endpoints for the VPN with the key and the first set of endpoints; and

a forwarding engine coupled with the control engine and the input/output module, the forwarding engine to dynamically establish the GRE tunnel with the first set of endpoints and the second set of endpoints and to process a set of traffic for the VPN.

16. The apparatus of claim 15 wherein the second set of endpoints are indexed by the key and the first set of endpoints.

17. The apparatus of claim 15 wherein to establish the GRE tunnel comprises:

to configure one of the second set of endpoints to one of the first set of endpoints; and

to indicate the key in a list of keys.

18. A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

retrieving a first set of endpoints of a generic routing encapsulation (GRE) tunnel with a generic routing encapsulation (GRE) tunnel name;

determining a second set of endpoints with the first set of endpoints and a key, the key corresponding to a virtual private network (VPN);

establishing an initiation point of the GRE tunnel with the first set of endpoints and the second set of endpoints;

transmitting the first set of endpoints and the key; and

transmitting a set of traffic over the GRE VPN.

19. The machine-readable medium of claim 18 wherein the establishing the initiation point of the GRE tunnel comprises configuring one of the second set of endpoints to one of the first set of endpoints.

20. The machine-readable medium of claim 18 further comprising:

receiving a second set of traffic for a second VPN, the second set of traffic indicating the GRE tunnel;

determining a third set of endpoints with a second key and the first set of endpoints, the second key corresponding to the second VPN;

configuring one of the third set of endpoints to one of the first set of endpoints;

transmitting the second key and the first set of endpoints; and

transmitting the second set of traffic.

21. A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

listening for a packet, the packet indicating a first set of endpoints for a generic routing encapsulation (GRE) tunnel and a key, the key corresponding to a virtual private network (VPN);

receiving the packet;

retrieving a second set of endpoints for the VPN with the first set of endpoints and the key;

establishing the GRE tunnel with the first set of endpoints and the second set of endpoints; and

processing a set of traffic over the GRE VPN.

22. The machine-readable medium of claim 21 wherein establishing the GRE tunnel comprises:

configuring one of the second set of endpoints to one of the first set of endpoints; and

maintaining the key in a list of keys.

23. The machine-readable medium of claim 21 further comprising:

receiving a second packet, the second packet indicating the first set of endpoints and a second key, the second key corresponding to a second VPN;

retrieving a third set of endpoints with the second key and the first set of endpoints;

receiving a second set of traffic; and

forwarding the second set of traffic to one of the third set of endpoints.

24. The machine-readable medium of claim 21 further comprising:

receiving a second packet, the second packet indicating a second key;

determining that the second key is not in a key list; and

ensuring that the second packet originated from an interior source.